Information Security Issues

Rob McKinney

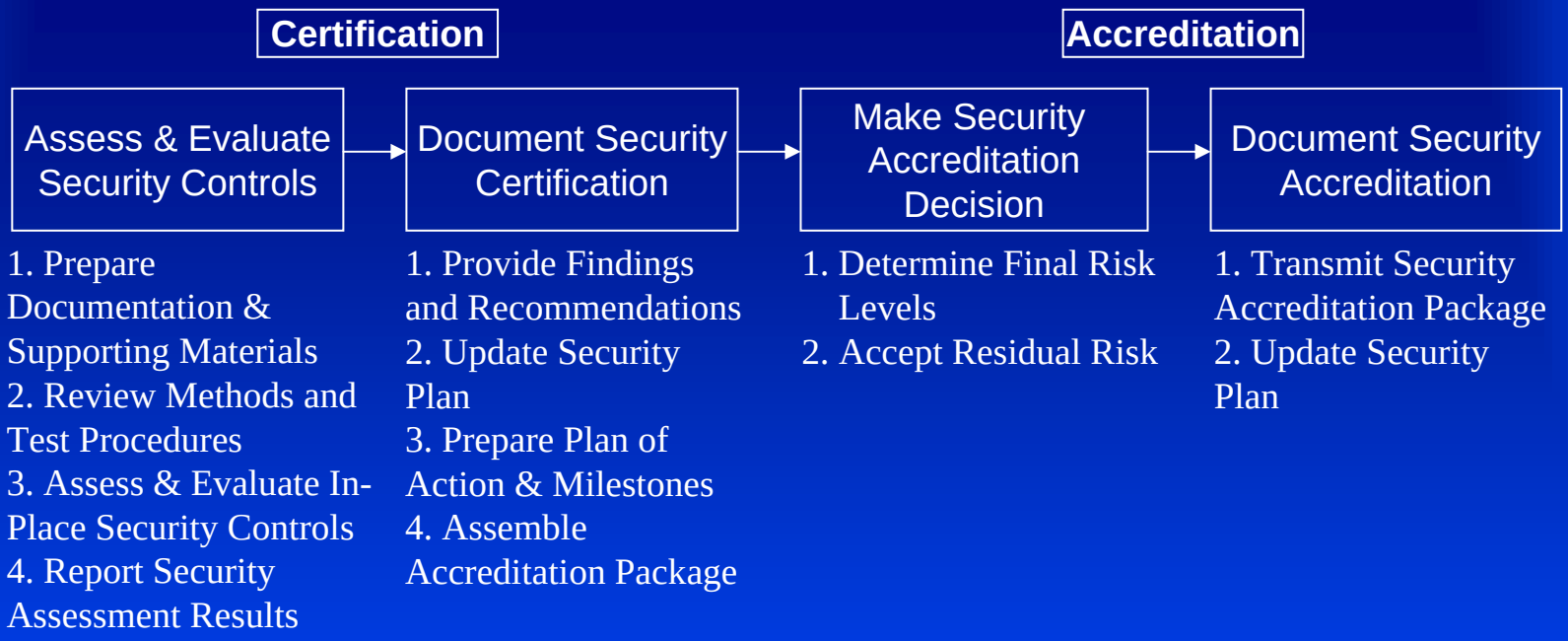
Topics

- Certification & Accreditation
- Training
- Managed Services

Certification & Accreditation

- Some requirements of process
- Risk assessments
  - Cost estimates
  - Alternative

Certification & Accreditation



Pilot program initiated to reduce the effort associated with developing and maintaining C&A documents

RA In-house vs. Outsourced

- Assumptions: 386 facilities (with: 100 – level1, 150 – level 2, 100 – level 3, and 36 – level 4);
- In-house
  - Centralized
  - Estimated total = $5.73M + some additional costs for training, equipment etc.
  - Decentralized cost is comparable to centralized although overall costs will likely be greater due to at least some duplication of items such as tools and training
- Outsourced
  - Centralized and decentralized have the same cost estimates to accomplish RA's however, a centralized structure may be able to negotiate lower costs due to volume
  - Estimated total = $8.4M

Nominal Entity Descriptions

- Level 1 – 50- users, simple LAN with associated hubs, perhaps one or two routers or switches, possibly a firewall
- Level 2 – 50 – 200 users, a small LAN with associated hubs, routers, and or switches, possibly a firewall and servers
- Level 3 – 200 – 700 users, one or two buildings with one or two LAN's and associated hubs, routers, and switches, one or two firewalls, various servers
- Level 4 – 700+ users, one to five buildings with separate LAN's possibly a small WAN and associated hubs, routers, and switches, one or more firewalls, various servers, e.g., email, web, DNS

Minimizing Costs

- Centralized capability
  - Spread over three-year period
  - Provides additional services, e.g.:
    - Infosec / adhoc systems training
    - Vulnerability remediation
    - Audit
- Use of *common information security controls* that can be applied to one or more Agency information systems
  - Assessments of common controls can be used to support C&A's of agency information systems where those controls have been applied
  - Example: RPMS – "type" C&A
- Possibility at the facility level:
  - Implement standards according to representative facilities
  - Conduct C&A's on representatives and apply to others

Minimizing Costs

- Common Infosec Controls: Facility Perspective
  - Would require development and implementation of standards / standard infosec controls; e.g., OS's, security appliances, applications, configurations
  - Cons: some initial costs of migrating to standards, loss of some autonomy with IT systems
  - Pros: meeting standards requirement, cost reductions through bulk purchases, sharing IT expertise, reduced maintenance and implementation costs, supports move to centralized automated patch management system and NOSC, significantly reduces costs associated with C&A's, e.g., conducting 4-12 C&A's every three years vs. hundreds

Infosec Training

- HHS / OPM requirements
- Immediate requirements
- Program

Training

- HHS Implementation of FISMA training requirement interpreted by OPM – provide infosec training for personnel with significant infosec responsibilities
  - Executives
  - Program and functional managers
  - Chief Information Officers (CIO)
  - IT security program managers
  - Auditors
  - Security-oriented personnel (e.g., system and network administrators, and system/application security officers)
  - IT function management and operations personnel

Training

- Immediate concern
  - Designated Accrediting Authority
  - Certification Agent
- 50% trained by 31 Mar 05
- 100% training by 1 Jun 05
- 84 DAA's – train with in-house resources
- 85 CA's – example training: 3 days - at Customer site, 25 students per class; cost per class = $15,753.33 + instructor per diem at government rate
  - Developing plan to meet requirements

Training

- IHS needs an Infosec Training Program to meet requirements – choices dependent upon HHS mandates
  - Vendor provided
    - On and off-site
  - In-house developed
    - Video conference
    - Web based
    - Distant learning
      - Blackboard type application
    - Trainer onsite
    - Train-the-trainer

Security Managed Services

- Requirement
- Options

Managed Services

- Changing architecture requires protection at each facility
  - Firewall / IPS
    - Anti-Virus, Anti-Spam, Web Filtering
- Implementation
  - In-house
  - Outsource
- Security Operations Center - Alerts – Incident Response support
  - In-house
    - Area or facility level
    - Centralized
  - Outsource - centralized

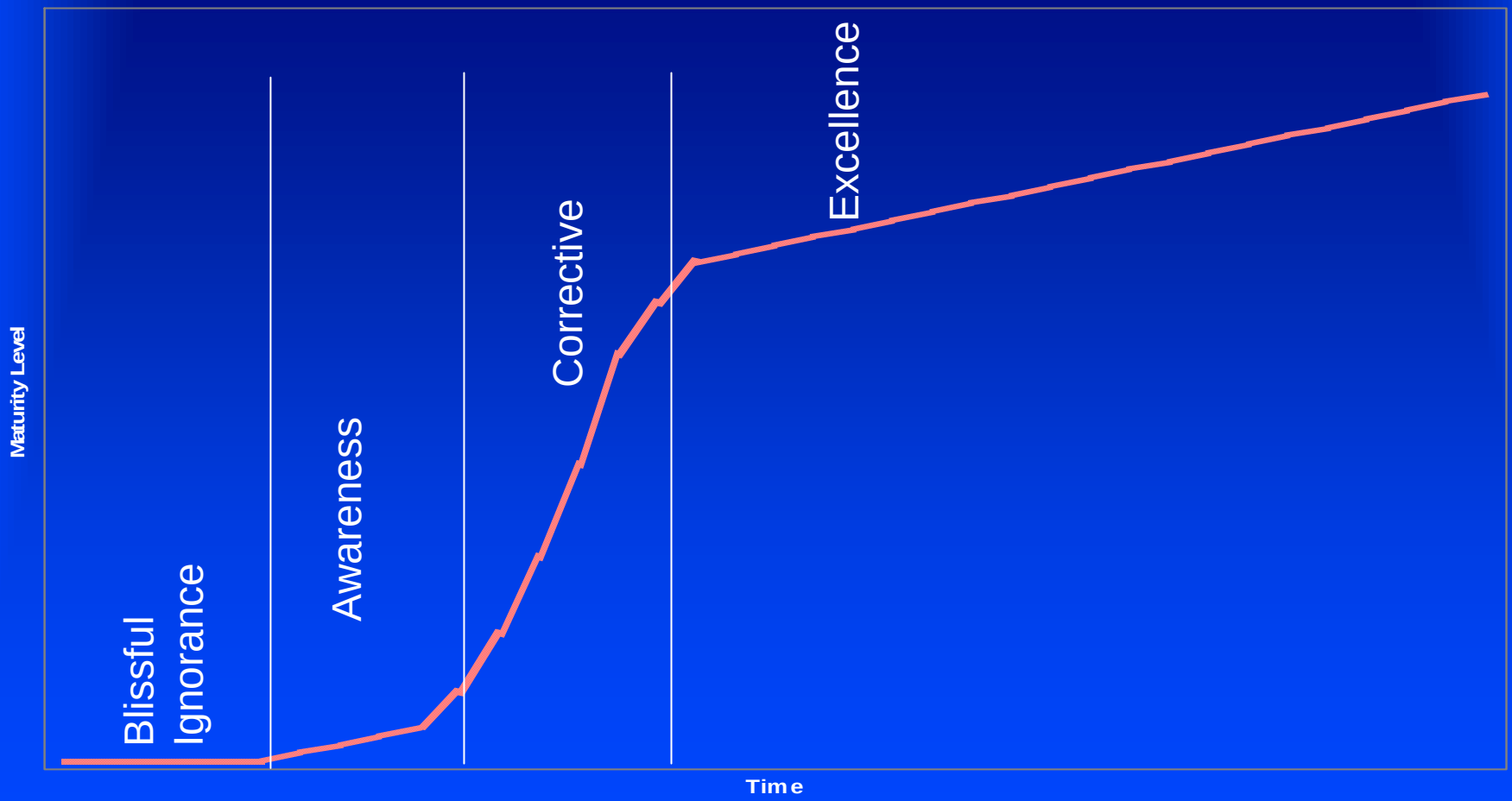
Managed Services

- Combined Network Operations Center and Security Operations Center – NOSC
  - HHS implementing capability
    - Could incorporate all OPDIVs
- Propose IHS implement
  - More effective

Managed Services

Total	Est. 1	Est. 2	Est. 3
Setup	$2.87M	$880,000	$561,600
Recurring	$2.36M	$2.72M	$3.02M
# facilities	400	200 small	200 FW
or devices		184 med	200 router
		16 large	
Cost/facility			
Setup	$7,187	$2,200	$2,700/FW
			$108/router
Recurring	$491	$300 small	$1,080/FW
/month		$800 med	$108/router
		$1,200 large	

Infosec Program Maturity



Summary

- Develop and implement standards
  - Conduct a few representative C&A's
- Provide DAA and CA training by June 2005
- Implement an Infosec Training Program
- Deploy security appliance
- Implement centralized combination network and security operations center